

DOI: <https://doi.org/10.32839/2304-5809/2019-4-68-83>  
 УДК 341(4-672ЄС)+(477)

**Ковінько Н.М.**

Національний юридичний університет імені Ярослава Мудрого

## ЕКСТРАТЕРИТОРІАЛЬНА ДІЯ GDPR: РИЗИКИ ДЛЯ УКРАЇНЦІВ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ УРЯДУ

**Анотація.** Стаття присвячена вивченню та аналізу нового Регламенту Європейського Союзу про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General data protection regulation / Загальний регламент по захисту даних) від 26 квітня 2016 року та проблем його впровадження в Україні. Досліджено понятійний апарат Регламенту, положення про екстра-територіальність його дії. Також Регламент проаналізовано в контексті можливості його застосування щодо фізичних та юридичних осіб України, запропоновано основні шляхи вдосконалення процесу адаптації українського законодавства про захист персональних даних до нових стандартів ЄС.

**Ключові слова:** Регламент ЄС 2016/679, контролер, оператор (процесор), екстра-територіальність, незалежний контролюючий орган.

**Kovin'ko Nataliia**

Yaroslav Mudryi National Law University

## EXTRA-TERRITORIAL ACTION OF GDPR: RISKS FOR UKRAINIANS AND PRACTICAL GUIDELINES FOR GOVERNMENT

**Summary.** The article is devoted to the study and analysis of the new European Union Regulation on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) of April 26, 2016 and its implementation problems in Ukraine. The conceptual apparatus of the Regulations, the position on the extraterritoriality of its action is investigated. The Regulation is also analyzed in the context of the possibility of its application to individuals and legal entities of Ukraine, the main ways of improving the process of adaptation of Ukrainian legislation on the protection of personal data to the new EU standards are proposed. In the article the author analyses not only the above mentioned Regulation, but also main laws of domestic Ukrainian legislation. She also compares definitions that are given in the Regulation with respective terms from Ukrainian laws in order to complete deep and full analysis of the main problems that can arise during implementing of GDPR at Ukraine. In particular, the author has compared the definitions of the “operator” and “controller” meaning the subjects who are entitled to process the personal data that are defined in the Regulation and the respective definition of such subject in Ukrainian laws. Moreover, article has a part describing the penalties that can be applied according to the Regulation and Ukrainian Code of Administrative Offences to those subjects who breach the rules of proceeding the personal data. Also article includes brief description of the measures that were taken at leading European countries in comply with the Regulation. On the grounds of such all-around research the author has identified the issues that can impact to the process of Regulation implementation at Ukraine and has suggested several steps to solve them successfully.

**Keywords:** EU Regulation 2016/679, controller, operator (processor), extraterritoriality, independent control body.

**Постановка проблеми.** У сучасних умовах масштаби збирання та обробки персональних даних надзвичайно зросли. Органи державної влади та юридичні особи приватного права, зараз, мають можливість здійснювати збір та обробку персональних даних в необмеженій кількості. Законодавством Європейського Союзу (далі – ЄС) визначається, що захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом. Так, статтею 8(1) Хартії фундаментальних прав Європейського Союзу і статтею 16(1) Договору про функціонування Європейського Союзу встановлено, що кожна особа має право на захист своїх персональних даних [1–2].

Раніше правові межі для захисту персональних даних у ЄС встановлювала Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (далі – Директива), однак вона не була обов'язковою, а встановлювала лише орієнтири, якими держави-члени мали послуговува-

тися при розробці національного законодавства [3]. У зв'язку із виникненням явища транскордонних потоків персональних даних нагальною стала потреба не просто у правовому регулюванні захисту персональних даних, а й у дієвому механізмі жорсткого примусу за порушення прав особи. Саме з цією метою 26 квітня 2016 року було затверджено Регламент ЄС про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних (General data protection regulation/Загальний регламент по захисту даних) (далі – Регламент, GDPR), який уже 25 травня 2018 року почав діяти [4].

У світлі яскраво вираженого євроінтеграційного напрямку розвитку України та активного прагнення долучитися до європейської спільноти, постало цілком очікуване питання: які ж проблеми можуть виникнути при імplementації Регламенту в українське законодавство? Актуальність цього дослідження обґрунтовується ще й тим, що відповідно до Регламенту, передача персональних даних за межі Європейського Союзу буде дозволена лише за умови достатнього

рівня захисту персональних даних, що забезпечується в країні, у яку здійснюється така передача. Крім того, відповідно до Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС від 25 жовтня 2017 року (далі – Угода), Україна мала удосконалити своє законодавство про захист персональних даних з метою приведення його у відповідність з Регламентом до 25 травня 2018 року [5]. На жаль, вчасно виконати вимоги Угоди у цій частині Україні не вдалося, проте очевидно, що для успішного подолання Україною шляху до євроінтеграції, імплементації положень GDPR в українське законодавство не уникнути.

**Аналіз останніх досліджень та публікацій.** Вивченням та аналізом питання захисту персональних даних займалися такі вітчизняні науковці як Баранов О.А., Мельник К.С., Серьогін С.А., Базанов О.Ю., Кохановська О.В., Оніщенко О.В., Пазюк А.В., Пилипчук В.Г., Брижко В.М.

**Виділення не вирішених раніше частин загальної проблеми.** Оскільки явище транскордонних потоків персональних даних стало великою проблемою з якою веде боротьбу все Європейське Співтовариство, а Україна не може вчасно виконати вимоги Угоди в частині захисту персональних даних, таким чином виникла необхідність у пошуку шляхів вирішення даної проблеми.

**Метою даної статті** є дослідження окремих теоретичних та практичних проблем захисту персональних даних, пов'язаних із прийняттям GDPR, визначення ключових правових вимог, які стосуються безпосередньо України та встановлення базових аспектів, необхідних для адаптації українського законодавства до нового законодавства ЄС з правового регулювання персональних даних.

Основні питання, на які спрямовано дослідження:

1. Яким чином правила, встановлені Регламентом ЄС, впливають на фізичних та юридичних осіб України?

2. Які принципові нововведення містить Регламент, порівняно із державним регулюванням захисту персональних даних в Україні?

3. Які дії на законодавчому рівні потрібно здійснити для подальшої адаптації положень України про захист персональних даних до законодавства ЄС?

**Виклад основного матеріалу.** Оскільки в епоху Big Data правовідносини виникають на перетині юрисдикцій, то персональні дані будь-якої особи, у тому числі громадянина України, можуть піддаватися обробці суб'єктами господарювання ЄС, США і т. д. відповідно до правил цих країн. Аналогічно, фізичні та юридичні особи України, надаючи послуги з через Інтернет суб'єктам персональних даних із держав-членів ЄС, можуть обробляти персональні дані таких осіб. Аналіз положень Регламенту дозволяє зробити висновок, що хоча Україна і не є державою-учасницею ЄС, але правила, закріплені GDPR, можуть стосуватися безпосередньо суб'єктів її юрисдикції. Так, відповідно до ст. 3 Регламенту GDPR має екстра-територіальну дію, тобто його положення поширюються не лише на держав-членів ЄС, а в конкретних визначених Регламентом випадках і на фізичних та юридичних осіб України: «...2. Цей

Регламент застосовують до опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, *контролером або оператором*, який має осідок *поза межами Союзу* (не є резидентом держави-учасниці ЄС)...» [4].

Для кращого розуміння змісту цієї норми та сфери її дії потрібно визначити, хто є контролером та/або оператором (процесором), відповідно до Регламенту Відповідь на це питання надана у пп. 7-8 ст. 4 Регламенту: «контролер» – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; «оператор» (процесор) – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера [4]. Отже, крім самих держав-членів ЄС, під дію Регламенту підпадають також «контролери» та «оператори», які:

– мають співробітників в ЄС;

– проводять кампанії, здійснюють дослідження, моніторинг суб'єктів ринку ЄС (електронна комерція, маркетинг і т.д.);

– здійснюють будь-яку діяльність, спрямовану на ринок ЄС (постачають товари та надають послуги громадянам ЄС на платній та безоплатній основі);

– використовують персональні дані громадян ЄС для здійснення вищевказаної діяльності.

Наступне питання – можливість притягнення порушників до відповідальності. Для того, аби положення про захист персональних даних діяли та застосовувалися на практиці, Регламент передбачив жорсткий примус та санкції за їх порушення. Найменша сума штрафу, відповідно до ст. 83 Регламенту, складає 20 млн євро або 4% від валового доходу контролера та/або оператора [4]. Для порівняння: відповідно до законодавства України, у сфері захисту персональних даних максимальна сума штрафу складає 34 тис. грн (ч. 5 ст. 18839 КУпАП). Отже, з урахуванням того, що фізичні та юридичні особи України можуть підпадати під екстериторіальну дію Регламенту, то чи можна притягти такого порушника до відповідальності та накладати санкції, передбачені Регламентом? На даний час в Україні чіткого механізму застосування штрафів відповідно до законодавства ЄС немає, і поки що не зрозуміло, як до відповідальності можна притягти порушників-фізичних та юридичних осіб України. Тим не менше, можна спрогнозувати, що порушення контролерами/операторами України положень GDPR може призвести до наступних варіантів розвитку подій:

1) відмова при відкритті закордонного банківського рахунку, якщо в базі даних буде наявна інформація про порушення фізичною чи юридичною особою України норм GDPR;

2) заборона суб'єкту права ЄС продовжувати потік або передачу даних в Україні (фактично – це фактично розірвання договірних відносин);

3) ті контролери/оператори України, які дотримуватимуться положень Регламенту, будуть більш конкурентоспроможним на ринку, оскільки їм більше довірятимуть користувачі та контрагенти з ЄС.

Отже, Регламент складений таким чином, щоб не тільки створити можливість застосування при-

мусу і санкцій до порушників, а й спрямований на створення таких умови, щоб суб'єкт, який діє на території ЄС, ретельно обирає контрагентів з обробки персональних даних поза територією ЄС.

Відповідно до Угоди, сторони домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [6]. Якщо на час дії Директиви 95/46/ЄС та перед підписанням Угоди про асоціацію України з ЄС було визнано, що механізм регулювання захисту персональних даних в Україні відповідає тогочасним стандартам ЄС, то новий Регламент у деякій мірі закріпив принципово нові – наприклад, Регламент у Главі 6 передбачає, що у всіх державах – членах ЄС та країнах, пов'язаних економічними відносинами з ними, мають бути створені спеціальні незалежні контролюючі органи (*Supervisory authority*) для контролю за дотриманням прав у сфері захисту персональних даних, розгляду скарг, застосування санкцій тощо [4]. Організаційно-правове та методологічне забезпечення покладається Регламентом на національні уповноважені органи контролю захисту персональних даних, що також мають бути незалежними, підпорядкованими закону та підзвітними парламенту.

Контроль за дотриманням законодавства у сфері обробки персональних даних згідно з Регламентом повинен здійснюватися і на місцевому рівні. Кожен контролер (оператор) на підприємствах та в організаціях з чисельністю працівників понад 250 осіб має вести облік діяльності з обробки персональних даних. Крім того на підприємствах, в організаціях або інших об'єднаннях усіх форм власності має бути призначений спеціаліст із захисту даних. У випадку ж якщо контролер або оператор знаходиться поза межами ЄС, він повинен призначити в письмовій формі представника в Союзі.

Якщо прослідкувати процес імплементації цього механізму на рівні держав-членів Європейського союзу, то можна звернути увагу на те, що в більшості з них діють спеціальні органи з контролю захисту персональних даних. В Ірландії, Ісландії, та Іспанії створені й діють Комісія Парламенту та Омбудсмен із захисту даних, які підзвітні парламенту. В Угорщині ці функції виконує Комісар із захисту інформації, який очолює інститут з питань захисту персональних даних та призначається рішенням Парламенту. У Франції створені Національна комісія з інформатики, склад якої обирається Парламентом, а також є посада Комісара із захисту персональних даних, який очолює агентство з питань захисту персональних даних призначається рішенням Прем'єр-міністра. У Швеції контроль за дотриманням законодавства про захист персональних даних покладений на Інспекційну раду та Омбудсмена із захисту даних, що також звітує перед парламентом [9].

Не можна сказати, що в Україні зовсім немає органів, уповноважених на виконання подібних функцій. Так, Законом повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. Із метою реалізації цих повноважень у структурі Секретаріату омбудсмена функціонує окремий

підрозділ, серед основних завдань якого – здійснення моніторингу застосування законодавства з питань захисту персональних даних, за результатами якого вживаються необхідні заходи. Однак, ці органи не є вузькоспеціалізованими і потребують модернізації [7].

Із урахуванням вищевикладеного аналізу основних нововведень Регламенту та короткого огляду існуючої системи захисту персональних даних в Україні, можна висунути наступні рекомендації, які послугують ефективному та повному впровадженню стандартів ЄС в нашій державі. Так, до базових та першочергових кроків адаптації можна віднести наступні:

1. затвердження та розробка Верховною Радою України ефективної програми державної політики щодо захисту персональних даних та здійснення парламентського контролю у цій сфері;

2. запровадження та закріплення інституту Уповноваженого з питань захисту персональних даних, основними функціями якого будуть забезпечення нагляду і контролю та удосконалення нормативно-правової бази з питань захисту персональних даних, а також взаємодія з уповноваженими органами ЄС та країн-членів ЄС з питань захисту даних;

3. створення спеціальних підрозділів із захисту персональних даних, які могли б діяти у складі Міністерства юстиції, наприклад;

4. покладення на Адміністрацію Державної служби спеціального зв'язку та захисту інформації України функції організації забезпечення технічного захисту персональних даних в Україні;

5. віднесення до компетенції Державного бюро розслідувань України проведення розслідування правопорушень, які стосуються захисту персональних даних;

6. створення окремих судових палат у складі апеляційних судів або створення спеціалізованого суду з питань захисту інформації (даних), де можна розглядати питання не тільки захисту персональних даних, а й порушень приватності життя, обігу публічної інформації, діяльності ЗМІ і т. д. [10];

7. запровадження в органах, установах, закладах, підприємствах та організаціях посад фахівців з питань захисту персональних даних або покладання цих функцій на окремих працівників цих організацій [4].

Підсумовуючи, можна сказати, що Регламент є принципово новим положенням законодавства ЄС щодо захисту персональних даних. На відміну від попередньої Директиви, GDPR встановлює чіткі та жорсткі правила, запроваджує дієвий механізм, який дозволить практично застосовувати принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних, незалежно від їхнього громадянства або місця проживання. Не зважаючи на відсутність в Україні статусу повноцінного члена ЄС, відповідно до Регламенту на нашу державу у конкретних випадках також поширюється дія GDPR. Це означає у свою чергу, що орієнтовані на європейський ринок суб'єкти господарювання України повинні детально пристосувати свою політику та процес обробки та збору персональних даних відповідно до GDPR, і мати на увазі, що тимчасові труднощі у встановленні шляху притягнення їх до від-

повідальності за Регламентом не є підставою для ігнорування відповідних норм. Так чи інакше, для порушників наставатимуть несприятливі наслідки у вигляді штрафів, розірвання вартісних контрактів із суб'єктами ЄС тощо.

Якщо говорити про проблему законодавчого врегулювання, то враховуючи принципову новизну багатьох положень та норм GDPR, потрібно розробляти та вносити суттєві зміни до ме-

ханізму регулювання та захисту персональних даних в Україні. Зокрема, необхідно посилити парламентський контроль у цій сфері, привести понятійний апарат українського законодавства у відповідність із законодавством ЄС, запровадити інституції, уповноважені на здійснення контролю та постійного моніторингу за станом захисту персональних даних, посилити санкції за порушення захисту персональних даних тощо.

## Список літератури:

1. Хартія фундаментальних прав Європейського Союзу від 07.12.2000 / База даних «Законодавство України». URL: [http://zakon.rada.gov.ua/go/994\\_524](http://zakon.rada.gov.ua/go/994_524)
2. Договір про функціонування Європейського Союзу від 07.02.1992, 25.03.1957 / База даних «Законодавство України». URL: [http://zakon.rada.gov.ua/go/994\\_b06](http://zakon.rada.gov.ua/go/994_b06)
3. Директива 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних / База даних «Законодавство України». URL: [http://zakon.rada.gov.ua/go/994\\_242](http://zakon.rada.gov.ua/go/994_242)
4. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679>
5. План заходів щодо імплементації Угоди про асоціацію між Україною та ЄС. URL: <https://www.kmu.gov.ua/ua/npas/pro-vikonannya-ugodi-pro-asociaciyu-mizh-ukrayinoyu-z-odniyeyi-storoni-ta-yevropejskim-soyuzom-yevropejskim-spivtovaristvom-z-atomnoyi-energiyi-i-yihnimi-derzhavami-chlenami-z-inshoyi-storoni>
6. Звіт «Про виконання Угоди про асоціацію між Україною та Європейським Союзом в 2016». URL: <https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/vikonannya-ugodi-pro-asociaciyu/zviti-pro-vikonannya-ugodi-pro-asociaciyu>
7. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI / Верховна Рада України. URL: <http://zakon.rada.gov.ua/go/2297-17>
8. Брижко В.М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3(18). С. 45.
9. Посібник з європейського права у сфері захисту персональних даних. URL: [https://www.echr.coe.int/Documents/Handbook\\_data\\_protection\\_UKR.pdf](https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf)
10. Гуз А.М. Навчальний посібник «Історія захисту інформації в Україні та провідних країнах світу». URL: <http://narodna-osvita.com.ua/2453-navchalniy-posbnik-storya-zahistu-nformacyi-v-ukrayin-ta-provdnih-krayinah-svtu-guz-a-m-skachati-chitati-onlayn.html>

## References:

1. Charter of Fundamental Rights of the European Union dated December 7, 2000 / Database "Legislation of Ukraine". URL: [http://zakon.rada.gov.ua/go/994\\_524](http://zakon.rada.gov.ua/go/994_524)
2. Treaty on the Functioning of the European Union dated February 7, 1992, 25.03.1957 / Database "Legislation of Ukraine". URL: [http://zakon.rada.gov.ua/go/994\\_b06](http://zakon.rada.gov.ua/go/994_b06)
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Database "Legislation of Ukraine". URL: [http://zakon.rada.gov.ua/go/994\\_242](http://zakon.rada.gov.ua/go/994_242)
4. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation). URL: <http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?Uri=CELEX:32016R0679>
5. Action Plan on Implementation of the Association Agreement between Ukraine and the EU. URL: <https://www.kmu.gov.ua/ua/npas/pro-vikonannya-ugodi-pro-asociaciyu-mizh-ukrayinoyu-z-odniyeyi-storoni-ta-yevropejskim-soyuzom-yevropejskim-spivtovaristvom-z-atomnoyi-energiyi-i-yihnimi-derzhavami-chlenami-z-inshoyi-storoni>
6. Report on the implementation of the Association Agreement between Ukraine and the European Union in 2016. URL: <https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/vikonannya-ugodi-pro-asociaciyu/zviti-pro-vikonannya-ugodi-pro-asociaciyu>
7. On Protection of Personal Data: Law of Ukraine dated 01.06.2010 No. 2297-VI / The Verkhovna Rada of Ukraine. URL: <http://zakon.rada.gov.ua/go/2297-17>
8. Bryzhko V.M. (2016). Modern bases of protection of personal data in European legal acts. *Information and right*, no. 3(18), p. 45.
9. European Legal Guide on the Protection of Personal Data. URL: [https://www.echr.coe.int/Documents/Handbook\\_data\\_protection\\_UKR.pdf](https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf)
10. Guz A.M. A manual "History of Information Protection in Ukraine and the Leading Countries of the World". URL: <http://narodna-osvita.com.ua/2453-navchalniy-posbnik-storya-zahistu-nformacyi-v-ukrayin-ta-provdnih-krayinah-svtu-guz-a-m-skachati-chitati-onlayn.html>